

GOVERNMENT OF THE REPUBLIC
OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



GOVERNEMENT DE LA
REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

21 May 2026

Advisory 146: Microsoft Defender Denial of Service Vulnerability

Release Date: 20th May 2026

Impact: **HIGH / CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-45498 is a medium-severity Denial of Service (DoS) vulnerability (CVSS 4.0) affecting Microsoft Defender and the Microsoft Malware Protection Engine. The vulnerability allows an attacker to cause the security service to become unavailable or unstable through local exploitation.

What are the systems affected?

The vulnerability affects:

- Microsoft Defender
- **Microsoft Malware Protection Engine** versions prior to:
 - **1.1.26040.8**
- Defender platform versions prior to:
 - **4.18.26040.7**

Affected environments may include:

- Windows 10 and Windows 11 endpoints
- Windows Server systems using Microsoft Defender
- Enterprise-managed Defender deployments

What does this mean?

Typical exploitation flow:

1. Initial local access obtained

- The attacker gains access to the target system through:
 - malware infection
 - compromised user account
 - phishing or other intrusion methods

2. Crafted input delivered to Defender

- Malicious files or specially crafted content are introduced to trigger Defender scanning behavior.

3. Defender engine instability triggered

- The Malware Protection Engine improperly handles the input.

4. Security service disruption

- Microsoft Defender may:
 - crash
 - stop responding
 - fail to scan files properly
 - temporarily lose protection capability

Mitigation process

CERTVU recommends the following:

Apply Microsoft Security Updates (Critical) immediately

Reference

1. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
2. <https://www.cve.org/CVERecord?id=CVE-2026-45498>
3. <https://nvd.nist.gov/vuln/detail/CVE-2026-45498>

